COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

Information Technology Security Standard

Virginia Information Technologies Agency (VITA)

ITRM PUBLICATION VERSION CONTROL

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Questions should be directed to VITA's Director for Policy Practice and Architecture (PPA) within the Information Technology Investment and Enterprise Solutions (ITIES) Directorate. PPA will issue a Change Notice Alert and post on the VITA Web site, provide an email announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions as well as other parties PPA considers interested in the change.

This chart contains a history of this ITRM publication's revisions.

Version	Date	Purpose of Revision
Original	12/07/2001	Base Document
Revision 1	07/01/2006	To update all sections of the Standard in accordance with changes to the *Code of Virginia* as well as incorporate emerging best practices.
	10/10/2006	To remove from section 2.1 (page 3) "Risk Response" that was erroneously left in the final version of this standard. Also, there are no requirements impacted by this correction.
Revision 2	7/1/07	Revision to align with changes (blue highlights) to the Code of Virginia and to document additional and substantively revised standards. The compliance date for these new and substantively revised standards is July 1, 2008.
Revision 3	10/30/2007	Revision to incorporate ITIB's directive (dated October 18, 2007) to change compliance date from July 2008 to November 1, 2007 for section 9.5.2 items 3 through 6.
Revision 4	07/24/08	Revision to align with changes (blue highlights) to the Code of Virginia, removed language in the scope section that excluded "Academic Instruction and Research" systems, and to document additional and revised standards. There is a new section for Application Security. The compliance date for these new and substantively revised standards is January 1, 2009 except for academic and research systems previously exempted, the compliance date shall be July 1, 2009.

Review Process

Technology Strategy and Solutions Directorate Review

N. Jerry Simonoff, VITA Director of Information Technology Investment and Enterprise Solutions (ITIES), and Chuck Tyger, Director for Policy, Practices, and Architecture Division (PPA) provided the initial review of the report.

Agency Online Review

The report was posted on VITA's Online Review and Comment Application (ORCA) for 30 days. All agencies, stakeholders, and the public were encouraged to provide their comments through ORCA. All comments were carefully evaluated and individuals that provided comments were notified of the action taken

PREFACE

Publication Designation
COV ITRM Standard SEC501-01

Subject
Information Technology Security

Effective Date
July 24, 2008

Compliance Date
January 1, 2009 – for new and revised requirements except for academic and research systems previously exempted, the compliance date shall be July 1, 2009.

.

Supersedes
COV ITRM Guideline SEC2001-01.1 dated December 7, 2001 (revision: 0).

Scheduled Review
One (1) year from effective date

Authority
Code of Virginia § 2.2-603(G)
(Authority of Agency Directors)

Code of Virginia, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information Technologies Agency; "VITA;"
Appointment of Chief Information Officer (CIO))

Code of Virginia, §2.2-2009
(Additional Powers of the CIO relating to security)

Code of Virginia, §2.2-2457
(Information Technology Investment Board)

Code of Virginia, §2.2-2827
(Restrictions on State employee access to information Infrastructure)

Code of Virginia, §2.2-3803
(Administration of systems including personnel information; Internet privacy policy)

Code of Virginia, §18.2-186.6
(Breach of personal information notification)

Scope
In general, this *Standard* is applicable to the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education (collectively referred to as "Agency"). This *Standard* is offered only as guidance to local government entities. Exemptions from the applicability of this *Standard* are defined in detail in Section 1.6.

In addition, *the Code of Virginia* § 2.2-2009, specifies that policies, procedures, and standards that address security audits (Section 2.7 of this *Standard*) apply only to *"all executive branch and independent agencies and institutions of higher education."* Similarly, *the Code of Virginia* § 2.2-603, specifies that requirements for reporting of information security incidents (Section 9.3.2.6 of the *Standard)* apply only to" *every department in the executive branch of state government."*

Purpose
To define the minimum requirements for each Agency's information technology security management program.

General Responsibilities
(Italics indicate quote from the Code of Virginia requirements)

Chief Information Officer
In accordance with *Code of Virginia* § 2.2-2009, the Chief Information Officer (CIO) is assigned the following duties: *"the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of electronic information"*

Chief Information Security Officer
The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of the Commonwealth of Virginia's information technology systems and data.

Judicial and Legislative Branches
In accordance with the *Code of Virginia* §2.2-2009: the: *"CIO shall work with representatives of the Chief Justice of the Supreme Court and Joint Rules Committee of the General Assembly to identify their needs."*

Information Technology Investment and Enterprise Solutions Directorate
In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the Information Technology Investment and Enterprise Solutions Directorate the

following duties: *Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions*."

Regulatory References

1. Health Insurance Portability and Accountability Act
2. Privacy Act of 1974
3. Children's Online Privacy Protection Act
4. Family Educational Rights and Privacy Act
5. Executive Order of Critical Infrastructure Protection
6. Federal Child Pornography Statute: 18 U.S.C. & 2252
7. Federal Rehabilitation Act of 1973, § 508
8. Bank Secrecy Act
9. Virginia Computer Crime Act, *Code of Virginia*, §18.2-152.3.,4., 5., and 6
10. Library of Virginia Records Management Program, *Code of Virginia*, Title 42.1, Chapter 7, sec 42.1-85
11. Federal Information Security Management Act (FISMA)
12. Office of Management and Budget (OMB) Circular A-130

International Standards

1. International Standard, Information Technology – code of practice for information security management, BS ISO/IEC 17799:2005.

Definitions

See Glossary

Related ITRM Policy

COV ITRM Policy SEC500-02: Information Security Policy.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Intent

The intent of the *Information Technology Security Standard* is to establish the baseline for information technology (IT) security controls that include, but are not limited to, the requirements of all statutes and best practices listed on pages iii and iv. These controls will provide protection of Commonwealth of Virginia (COV) IT systems and data.

This *Standard* defines the minimum acceptable level of IT security for the COV, and Agencies must implement an IT security program that complies with this *Standard*. Agencies may implement their own IT security standards, based on IT security needs specific to their environments and commensurate with sensitivity and risk; agency IT security standards, however, must provide protection of the agency's IT systems and data equal to or greater than the requirements defined in this document. As used in this *Standard*, sensitivity encompasses the elements of confidentiality, integrity, and availability. See Section 2.5 for additional detail on sensitivity.

The COV IT Security Program consists of the following set of components:

- Risk Management
- IT Contingency Planning
- IT Systems Security
- Logical Access Control
- Data Protection
- Facilities Security
- Personnel Security
- Threat Management
- IT Asset Management

These components provide a framework to allow Agencies to accomplish their missions in a safe and secure technology environment. In addition, they provide a basis for each agency's IT security program. Each component listed above contains requirements that, together, comprise this *Information Technology Security Standard*.

This *Standard* recognizes that Agencies may procure IT equipment, systems, and services covered by this *Standard* from third parties. In such instances, Agency Heads remain accountable for maintaining compliance with this *Standard* and Agencies must enforce these compliance requirements through documented agreements with third-party providers. Similarly, VITA customer Agencies must provide VITA with information concerning their IT security requirements to enable VITA to meet the requirements of this *Standard* on their behalf.

1.2 Organization of this *Standard*

The nine components of the COV IT Security Program (listed in section 1.1, above) provide the organizational framework for this *Standard*. Each component consists of one or more sections composed of:

- A **Purpose** statement that provides a high-level description of the component or subcomponent and its importance in the COV IT Security Program;
- **Requirements** that are mandatory technical and/or programmatic activities for a specific area of the COV IT Security Program;

- **Notes**, which provide rationale and explanation regarding the requirements; and
- **Examples**, which describe ways in which Agencies might meet the requirements. These examples do not and should not be interpreted to suggest an appropriate course of action for particular COV agencies, personnel, systems, or facilities.

1.3 Roles and Responsibilities

Descriptions of key IT security roles and responsibilities are included in the current version of the *Information Technology Security Policy* (COV ITRM Policy SEC500). Each agency must maintain an organization chart that depicts the reporting structure of employees with specific responsibilities for the security of IT systems and data and their specific IT security roles and responsibilities.

1.4 IT Security Program

Each agency shall establish, document, implement, and maintain its IT security program appropriate to its business and technology environment in compliance with this *Standard*. In addition, because resources that can reasonably be committed to protecting IT systems are limited, each agency must implement its IT security program in a manner commensurate with sensitivity and risk.

1.5 Exceptions to Security Requirements

The Chief Information Security Officer of the Commonwealth (CISO) must approve exceptions to this Standard. For each exception, the requesting agency shall document:

- The business need,
- The scope and extent,
- Mitigating safeguards,
- The specific duration, and
- Agency Head approval.

If the CISO denies a request for an exception to this *Standard*, the agency requesting the exception may appeal the denial to the Chief Information Officer of the Commonwealth (CIO) through the CISO. The form that Agencies must use to document such exception requests is included as the Appendix to this document.

1.6 Exemptions from Applicability

The following are explicitly exempt from complying with the requirements defined in this document:

a. Systems under development and/or experimental systems that do not create additional risk to production systems
b. Surplus and retired systems

2. RISK MANAGEMENT

2.1 Purpose

Risk Management delineates the steps necessary to identify, analyze, prioritize, and mitigate risks that could compromise IT systems. This section defines requirements in the following areas:

- IT Security Roles and Responsibilities
- Business Impact Analysis
- IT System and Data Sensitivity Classification
- Sensitive IT System Inventory and Definition
- Risk Assessment
- IT Security Audits

2.2 IT Security Roles and Responsibilities

2.2.1 Purpose

IT Security Roles and Responsibilities requirements identify the steps necessary to establish formal roles and assign responsibilities to manage and protect the security of IT systems.

2.2.2 Requirements

Each Agency Head shall:

1. Designate an Information Security Officer (ISO) for the agency, and provide the person's name, title, and contact information to the CISO via email to VITASecurityServices@vita.virginia.gov no less than biennially. The Agency Head is strongly encouraged to designate at least one backup for the ISO. Agencies with multi-geographic locations or specialized business units should also consider designating deputy ISOs as needed.

Each Agency Head or designated ISO shall:

1. Assign individuals to the roles described in the current version of the *Information Technology Security Policy* (COV ITRM Policy SEC500).

2. Document the responsibilities of the designee for each role identified.

3. Review System Security Plans (Section 4.2) for all sensitive agency IT systems (Section 2.4) and:

    a. Approve those System Security Plans that provide adequate protections against IT security risks; or
    b. Disapprove System Security Plans that do not provide adequate protections against IT security risks, and require that the System Owner implement additional security controls on the IT system to provide adequate protections against IT security risks.

4. Prevent conflict of interests and adhere to the security concept of separation of duties by assigning roles so that:
    a. The ISO is not a System Owner or a Data Owner except in the case of compliance systems for IT Security;
    b. The System Owner and the Data Owner are not System Administrators for IT systems or data they own; and

c. The ISO, System Owners, and Data Owners are COV employees.

Notes:

- Other roles can be assigned to contractors. For roles assigned to contractors, the contract language shall include specific responsibility and background check requirements.
- The System Owner can own multiple IT systems.
- Data Owners can own data on multiple IT systems.
- System Administrators can assume responsibility for multiple IT systems.

5. Review the position descriptions of all employees assigned to IT security roles annually, or more often as necessary, and verify that the position descriptions accurately reflect assigned IT security duties and responsibilities.

2.3 Business Impact Analysis

2.3.1 Purpose

Business Impact Analysis (BIA) delineates the steps necessary for Agencies to identify their business functions, identify those agency business functions that are essential to an agency's mission, and identify the resources that are required to support these essential agency business functions.

Note: The requirements below address only the IT aspects of BIA and **do not** require that agencies develop a BIA separate from that which they develop to meet the BIA requirements specified by the Virginia Department of Emergency Management (VDEM). Agencies should create a single BIA, which meets both the requirements of this *Standard*, and those specified by VDEM, and should consult the VDEM *Continuity of Operation Planning Manual* for non-IT related BIA requirements.

2.3.2 Requirements

Each agency shall:

1. Require the participation of System Owners and Data Owners in the development of the agency's BIA.

2. Identify agency business functions.

3. Identify essential business functions.

   Note: A business function is essential if disruption or degradation of the function prevents the agency from performing its mission, as described in the agency mission statement.

4. Identify dependent functions. Determine and document any additional functions on which each essential business function depends. These dependent functions are essential functions as well.

5. For each essential business function:

   - Determine and document the required Recovery Time Objectives (RTO) for each essential business function, based on agency and COV goals and objectives.

- Determine and document the Recovery Point Objectives (RPO) for each essential business function.

- Identify the IT resources that support each essential business function.

6. Use the IT information documented in the BIA report as a primary input to IT System and Data Sensitivity Classification (Section 2.4), Risk Assessment (Section 2.6), and IT Contingency Planning (Section 3).

7. Conduct periodic review and revision of the agency BIA, as needed, but at least once every three years.

2.4 IT System and Data Sensitivity Classification

2.4.1 Purpose

IT System and Data Sensitivity Classification requirements identify the steps necessary to classify IT systems and data according to their sensitivity with respect to the following three criteria:

- Confidentiality, which addresses sensitivity to unauthorized disclosure;
- Integrity, which addresses sensitivity to unauthorized modification; and
- Availability, which addresses sensitivity to outages.

Sensitive Data is any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled. Data sensitivity is directly proportional to the materiality of a compromise of the data with respect to these criteria. Agencies must classify each IT system by sensitivity according to the most sensitive data that the IT system stores, processes, or transmits.

2.4.2 Requirements

Each agency ISO shall:

1. Identify or require that the Data Owner identify the type(s) of data handled by each agency IT system.

2. Determine or require that the Data Owner determine whether each type of data is also subject to other regulatory requirements.

   Example: Some COV IT systems may handle data subject to legal or business requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA); IRS 1075; the Privacy Act of 1974; Payment Card Industry (PCI); the Rehabilitation Act of 1973, § 508, Federal National Security Standards, etc.

3. Determine or require that the Data Owner determine the potential damages to the agency of a compromise of confidentiality, integrity or availability of each type of data handled by the IT system, and classify the sensitivity of the data accordingly.

   Example: Data Owners should construct a table similar to the following table. Data Owners must classify sensitivity requirements of all types of data. The following table is only an illustration.

System ID: ABC123	Sensitivity Criteria		
Type of Data	**Confidentiality**	**Integrity**	**Availability**
HR Policies	Low	High	Moderate
Medical Records	High	High	High
Criminal Records	High	High	High

Table 1: Sample Sensitivity Analysis Results

4. Any data type with one or more HIGH sensitivity rating in any of the three classifications shall be classified "sensitive" for the purposes of this standard.

   Note: Agencies should consider classifying IT systems as sensitive even if a type of data handled by the IT system has a sensitivity of moderate on the criteria of confidentiality, integrity, and availability.

5. Review IT system and data classifications with the Agency Head or designee and obtain Agency Head or designee approval of these classifications.

6. Verify and validate that all agency IT systems and data have been classified for sensitivity.

7. Communicate approved IT system and data classifications to System Owners, Data Owners, and end-users.

8. Require that the agency prohibit posting any data classified as sensitive with respect to confidentiality on a public web site, ftp server, drive share, bulletin board or any other publicly accessible medium. unless a written exception is approved by the Agency Head identifying the business case, risks, mitigating logical and physical controls, and any residual risk.

9. Use the information documented in the sensitivity classification as a primary input to the Risk Assessment process (Section 2.6).

2.5 Sensitive IT System Inventory and Definition

2.5.1 Purpose

Sensitive IT System Inventory and Definition requirements identify the steps in listing and marking the boundaries of sensitive IT systems in order to provide cost-effective, risk-based security protection for IT systems, for the agency as a whole, and for the COV enterprise.

2.5.2 Requirements

Each agency shall:

1. Document each sensitive IT system owned by the agency, including its ownership and boundaries, and update the documentation as changes occur.

Note: Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner for the purposes of this *Standard,* upon request, the CIO of the Commonwealth will determine the System Owner.

2. Assign a System Owner, Data Owner(s), and System Administrator(s) for each agency-owned sensitive IT system.

   Note: A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a designated System Owner.

3. Maintain or require that its service provider maintain updated network diagrams.

2.6 Risk Assessment

2.6.1 Purpose

Risk Assessment requirements delineate the steps Agencies must take for each IT system classified as sensitive to:

- Identify potential threats to an IT system and the environment in which it operates;
- Determine the likelihood that threats will materialize;
- Identify and evaluate vulnerabilities; and
- Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.

Note: The Risk Assessment (RA) required by this *Standard* differs from the RA required by the current version of the *Project Management Standard* (COV ITRM Standard GOV2004). This *Standard* requires an RA based on operational risk, while the *Project Management Standard* requires an RA based on project risk. Many of the RA techniques described in the *Project Management Standard*, however, may also be applicable to the RA required by this *Standard*.

2.6.2 Requirements

For each IT system classified as sensitive, the data owning agency shall:

1. Conduct a formal RA of the IT system, as needed, but not less than once every three years.

2. Conduct an annual self-assessment to determine the continued validity of the formal RA.

   Note: In addition, in Agencies that own both sensitive IT systems and IT systems that are exempt from the requirements of this *Standard*, the agency's RAs must include consideration of the added risk to sensitive IT systems from the exempt IT systems.

3. Prepare a report of each RA that includes, at a minimum, identification of all vulnerabilities discovered during the assessment, and an executive summary, including major findings and risk mitigation recommendations.

2.7 IT Security Audits

2.7.1 Purpose

IT Security Audit requirements define the steps necessary to assess whether IT security controls implemented to mitigate risks are adequate and effective.

Note: In accordance with *the Code of Virginia* § 2.2-2009, the requirements of this section apply only to *"all executive branch and independent agencies and institutions of higher education."*

2.7.2 Requirements

For each IT system classified as sensitive, the data owning agency shall:

1. Require that the IT systems undergo an IT Security Audit as required by and in accordance with the current version of the *IT Security Audit Standard* (COV ITRM Standard SEC502).

2. Assign an individual to be responsible for managing IT Security Audits.

3. IT CONTINGENCY PLANNING

3.1 Purpose

IT Contingency Planning delineates the steps necessary to plan for and execute recovery and restoration of IT systems and data if an event occurs that renders the IT systems and/or data unavailable. This component of the COV IT Security Program defines requirements in the following three areas:

- Continuity of Operations Planning
- Disaster Recovery Planning
- IT System Backup and Restoration

3.2 Continuity of Operations Planning

3.2.1 Purpose

COV Continuity of Operations Planning requirements are defined by VDEM. This section addresses only the Continuity of Operations Planning requirements for IT systems and data. Agencies should consult the *Continuity of Operations Planning Manual* published by VDEM for non-IT related requirements that address all essential business functions. The agency's overall Continuity of Operations Plan (COOP) should include the manual processing procedures for critical functions that users can follow until the agency restores operations, as appropriate.

These Continuity of Operations Planning requirements identify the steps necessary to provide continuity for essential agency IT systems and data through the development, implementation, exercise, and maintenance of the IT component of Continuity of Operations Plans.

3.2.2 Requirements

Each agency shall:

1. Designate an employee to collaborate with the agency Continuity of Operations Plan (COOP) coordinator as the focal point for IT aspects of COOP and related Disaster Recovery planning activities.

   Note: Designation of an agency COOP coordinator is included in the COOP planning requirements issued by VDEM.

2. Based on BIA and RA results, develop agency COOP IT-related documentation which identifies:

a. Essential business functions that require restoration and the Recovery Time Objective (RTO) for each;
b. Recovery requirements for IT systems and data needed to support the essential business functions; and
c. Personnel contact information and incident notification procedures.

Note: The COOP should be protected as sensitive data and stored at a secure off-site location.

3. Require an annual exercise (or more often as necessary) of IT COOP components to assess their adequacy and effectiveness.

4. Require review and revision of IT COOP components following the exercise (and at other times as necessary).

3.3 IT Disaster Recovery Planning

3.3.1 Purpose

IT Disaster Recovery Planning is the component of Continuity of Operations Planning that identifies the steps necessary to provide for restoring essential business functions on a schedule that support agency mission requirements. These steps lead to the creation of an IT Disaster Recovery Plan (DRP).

3.3.2 Requirements

Each agency shall:

1. Based on the COOP, develop and maintain an IT DRP, which supports the restoration of essential business functions.

2. Require approval of the IT DRP by the Agency Head.

3. Require periodic review, reassessment, testing, and revision of the IT DRP to reflect changes in essential business functions, services, IT system hardware and software, and personnel.

4. Establish communication methods to support IT system users' local and remote access to IT systems, as necessary.

3.4 IT System and Data Backup and Restoration

3.4.1 Purpose

IT System and Data Backup and Restoration requirements identify the steps necessary to protect the availability and integrity of COV data documented in backup and restoration plans.

3.4.2 Requirements

For every IT system identified as sensitive, each agency shall or shall require that its service provider implement backup and restoration plans to support restoration of systems and data in accordance with agency requirements. At a minimum, these plans shall address the following:

1. Secure off-site storage for backup media.

2. Store off-site backup media in an off-site location that is geographically/separate and distinct from the primary location.
3. Performance of backups only by authorized personnel.
4. Review of backup logs after the completion of each backup job to verify successful completion.
5. Approval of backup schedules of a system by the System Owner.
6. Approval of emergency backup and operations restoration plans by the System Owner.
7. Protection of any backup media that is sent off site (physically or electronically), or shipped by the United States Postal Service or any commercial carrier, in accordance with agency requirements.
8. Authorization and logging of deposits and withdrawals of all media that is stored off-site.
9. Retention of the data handled by an IT system in accordance with the agency's records retention policy.
10. Management of electronic information in such a way that it can be produced in a timely and complete manner when necessary, such as during a legal discovery proceeding.

4. IT SYSTEMS SECURITY

4.1 Purpose

IT Systems Security requirements delineate steps to protect IT systems in the following five areas:

- IT System Security Plans
- IT System Hardening
- IT Systems Interoperability Security
- Malicious Code Protection
- IT Systems Development Life Cycle

4.2 IT System Security Plans

4.2.1 Purpose

IT System Security Plans document the security controls required to demonstrate adequate protection of IT systems against IT security risks.

4.2.2 Requirements

Each System Owner of a sensitive IT system shall:

1. Document an IT System Security Plan for the IT system based on the results of the risk assessment. This documentation shall include a description of:
    a. All IT existing and planned IT security controls for the IT system, including a schedule for implementing planned controls;
    b. How these controls provide adequate mitigation of risks to which the IT system is subject.

2. Submit the IT System Security Plan to the Agency Head or designated ISO for approval.

3. Plan and document additional IT security controls for the IT system if the Agency Head or designated ISO disapproves the IT System Security Plan, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.

4. Update the IT System Security Plan every three years, or more often if necessary, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.

4.3 IT System Hardening

4.3.1 Purpose

IT System Hardening requirements delineate technical security controls to protect IT systems against IT security vulnerabilities.

4.3.2 Requirements

Each agency shall or shall require that its service provider:

1. Identify, document, and apply appropriate baseline security configurations to agency IT systems, regardless of their sensitivity.
2. Identify, document, and apply more restrictive security configurations for sensitive agency IT systems, as necessary.

   Note: Agencies may develop agency-specific baseline security configuration standards or may elect to use baseline security configuration standards that are publicly available, such as those developed by the Center for Internet Security (www.cisecurity.org).
3. Maintain records that document the application of baseline security configurations.
4. Review and revise all security configuration standards annually, or more frequently, as needed.

   Note: Agencies should establish a process to review and catalog applicable security notifications issued by equipment manufacturers, bulletin boards, security-related Web sites, and other security venues, and establish a process to update security baseline configuration standards based on those notifications.
5. Reapply all security configurations to agency-owned IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.
6. Require periodic vulnerability scanning of IT systems in a manner commensurate with sensitivity and risk, to verify whether security configurations are in place and if they are functioning effectively.

7. Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.

4.4 IT Systems Interoperability Security

4.4.1 Purpose

IT System Interoperability Security requirements identify steps to protect data shared with other IT systems.

4.4.2 Requirements

For every sensitive agency-owned IT system, the agency shall require or shall specify that its service provider require:

1. The System Owner, in consultation with the Data Owner, document IT systems with which data is shared. This documentation shall include:

    a. The types of shared data;
    b. The direction(s) of data flow; and
    c. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator.

2. The System Owners of the IT systems which share data develop a written agreement that delineates IT security requirements for each interconnected IT system and for each type of data shared.

3. The System Owners of the IT systems that share data inform one another regarding other IT systems with which their IT systems interconnect or share data, and inform one another prior to establishing any additional interconnections or data sharing.

4. The written agreement specify if and how the shared data will be stored on each IT system.

5. The written agreement specify that System Owners of the IT systems that share data acknowledge and agree to abide with any legal requirements (i.e., HIPAA) regarding handling, protection, and disclosure of the shared data.

6. The written agreement maintains each Data Owner's authority to approve access to the shared data.

7. The System Owners approve and enforce the agreement.

4.5 Malicious Code Protection

4.5.1 Purpose

Malicious Code Protection requirements identify controls to protect IT systems from damage caused by malicious code.

4.5.2 Requirements

Each agency shall, or shall require that its service provider:

1. Prohibit all IT system users from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spy-ware, keystroke loggers, phishing software, Trojan horses, etc.).

2. Prohibit all IT system users from knowingly propagating malicious programs including opening attachments from unknown sources.

3. Provide malicious program detection, protection, eradication, logging, and reporting capabilities.

4. Provide malicious code protection mechanisms on multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms.

   Example: An agency may elect to provide protection against malicious code transmitted via email on the email servers and on the desktop.

5. Require malicious program protection that:

   a. Eliminates or quarantines malicious programs that it detects;
   b. Provides an alert notification;
   c. Automatically and periodically runs scans on memory and storage devices;
   d. Automatically scans all files retrieved through a network connection, modem connection, or from an input storage device;
   e. Allows only authorized personnel to modify program settings; and
   f. Maintains a log of protection activities.

6. Provide the ability to eliminate or quarantine malicious programs in email messages and file attachments as they attempt to enter the agency's email system.

7. Provide the ability for automatic download of definition files for malicious code protection programs whenever new files become available, and propagate the new files to all devices protected by the malicious code protection program.

8. Require all forms of malicious code protection to start automatically upon system boot.

9. Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.

10. Provide procedures that instruct administrators and IT system users on how to respond to malicious program attacks, including shutdown, restoration, notification, and reporting requirements.

11. Require use of only new media (e.g., diskettes, CD-ROM) or sanitized media for making copies of software for distribution.

12. Prohibit the use of common use workstations and desktops (e.g., training rooms) to create distribution media.

13. By written policy, prohibit the installation of software on agency IT systems until the software is approved by the Information Security Officer (ISO) or designee and, where practicable, enforce this prohibition using automated software controls, such as Active Directory security policies.

14. Establish Operating System (OS) update schedules commensurate with sensitivity and risk.

4.6 IT Systems Development Life Cycle Security

4.6.1 Purpose

IT Systems Development Life Cycle Security requirements document the security-related activities that must occur in each phase of the development life cycle (from project definition through disposal) for agency-owned IT application systems.

4.6.2 Requirements

Each agency shall:

1. Incorporate IT security requirements in each phase of the life cycle, as well as for each modification proposed for the IT application system in each stage of its life cycle.

Project Initiation

2. Perform an initial risk analysis based on initial requirements and the business objectives to provide high-level security guidelines for the system developers.
3. Classify the types of data (see Section 2.4) that the IT system will process and the sensitivity of proposed IT system.
4. Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.
5. Develop an initial IT System Security Plan (see Section 4.2) that documents the IT security controls that the IT system will enforce to provide adequate protection against IT security risks.

Project Definition

6. Identify, develop, and document IT security requirements for the IT system during the Project Definition phase.
7. Incorporate IT security requirements in IT system design specifications.
8. Verify that the IT system development process designs, develops, and implements IT security controls that meet the IT security requirements in the design specifications.
9. Update the initial IT System Security Plan to document the IT security controls included in the design of the IT system to provide adequate protection against IT security risks.
10. Develop IT security evaluation procedures to validate that IT security controls developed for a new IT system are working properly and are effective.

    Note: Some IT security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until after deployment of the IT system.

Implementation

11. Execute the IT security evaluation procedures to validate and verify that the functionality described in the specification is included in the product.

    Note: Results should be documented in a report, including identification of controls that did not meet design specifications.

12. Conduct a RA (see Section 2.6) to assess the risk level of the IT application system.

13. Require that the IT system comply with all relevant Risk Management requirements in Section 2 of this document.

14. Update the IT System Security Plan to document the IT security controls included in the IT system as implemented to provide adequate protection against IT security risks, and comply with the other requirements of Section 4.2 of this document.

Disposition

15. Require retention of the data handled by an IT system in accordance with the agency's records retention policy prior to disposing of the IT system.

16. Require that electronic media is sanitized prior to disposal, as documented in Section 6.2, so that all data is removed from the IT system.

17. Verify the disposal of hardware and software in accordance with the current version of the *Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard* (COV ITRM Standard SEC514).

4.7 Application Security

4.7.1 Purpose

Application security requirements define the high level specifications for securely developing and deploying Commonwealth applications.

4.7.2 Requirements

Each agency ISO is accountable for ensuring the following steps are followed and documented:

Application Planning

- Data Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data. (Section 2.4)

- Risk Assessment – If the data classification identifies the system as sensitive, a risk assessment shall be conducted before development begins and after planning is complete. (Section 2.6.2)

- Security Requirements – Identify and document the security requirements of the application early in the development lifecycle. For a sensitive system, this shall be done after a risk assessment is completed and before development begins.

- Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication and access control, and logging requirements.

- Security shall be addressed at all life cycle stages of the software development lifecycle (SDLC).

Application Development

The following requirements represent a minimal set of coding practices, which shall be applied to all applications that utilize un-trusted data.

- Input Validation – Validate input from all sources. Input validation to be tested should always consider expected and unexpected input, and not block input based on arbitrary criteria.

- Default deny – Access control should be based on specific permission rather than exclusion. By default all access should be denied.

- Principle of Least Privilege – All processes should be performed with the least set of privileges required to complete the process.

- Quality Assurance – Quality assurance is one of the single most effective means of identifying and eliminating software vulnerabilities. Internal testing shall include at least one of the following: penetration testing, fuzz testing, or source code auditing. External source code auditing and/or penetration testing shall be conducted commensurate with sensitivity and risk.

  Note: Source code auditing techniques include:

  - Manual code review can identify vulnerabilities as well as functional flaws, but most companies do not have the skilled security resources or time available within the software lifecycle that a manual code review requires, and therefore many companies who decide to perform manual code reviews can only analyze a small portion of their applications.
  - Application penetration testing tries to identify vulnerabilities in software by launching as many known attack techniques as possible on likely access points in an attempt to bring down the application or the entire system.
  - Automated source code analysis tools make the process of manual code review more efficient, affordable, and achievable. This technique of code audit results in significant reduction of analysis time, actionable metrics, significant cost savings, and can be integrated into all points of the development life cycle.

Production and Maintenance

- Applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening (Section 4.3.2).

Applications classified as sensitive shall at a minimum have annual vulnerability assessments run against the applications and supporting server infrastructure and when any significant change to the environment or application has been made. More frequent vulnerability assessments may be done commensurate with sensitivity and risk.

5. LOGICAL ACCESS CONTROL

5.1 Purpose

Logical Access Control requirements delineate the steps necessary to protect IT systems and data by verifying and validating that users are who they say they are and that they are permitted to use the IT systems and data they are attempting to access. Users are accountable for any activity on the system performed with the use of their account. This component of the COV IT Security Program defines requirements in the following three areas:

- Account Management
- Password Management
- Remote Access

5.2 Account Management

5.2.1 Purpose

Account Management requirements identify those steps necessary to formalize the process of requesting, granting, administering, and terminating accounts. Agencies should apply these Account Management practices to all accounts on IT systems, including accounts used by vendors and third parties.

The requirements below distinguish between internal and customer-facing IT systems. Internal IT systems are designed and intended for use only by COV employees, contractors, and business partners; customer-facing IT systems are designed and intended for use by agency customers and by members of the public. COV employees, contractors, and business partners may also use customer-facing IT systems.

5.2.2 Requirements

Each agency shall or shall require that its service provider document formal account management practices for requesting, granting, administering, and terminating accounts. At a minimum, these practices shall include the following components:

For all internal and customer-facing IT systems:

1. Grant IT system users' access to IT systems and data based on the principle of least privilege.

2. Define authentication and authorization requirements, based on sensitivity and risk.

3. Establish policies and procedures for approving and terminating authorization to IT systems.

4. Require requests for and approvals of emergency or temporary access to all sensitive IT systems that:

    a. Are documented according to standard practice and maintained on file;
    b. Include access attributes for the account.
    c. Are approved by the System Owner and communicated to the ISO; and
    d. Expire after a predetermined period, based on sensitivity and risk.

5. Based on risk, consider use of second-factor authentication, such as tokens and biometrics, for access to sensitive IT systems.

6. Provide for, review at a consistent frequency, relative to sensitivity and risk, of all user accounts for all IT systems to assess the continued need for the accounts.

7. Notify the System Administrator when IT system user accounts are no longer required, or when an IT system user's access level requirements change.

8. Prohibit the use of guest and shared accounts on sensitive IT systems..

9. Prohibit the displaying of user's last name in the logon screen.

10. Lock an account automatically if it is not used for a predefined period.

11. Disable unneeded accounts.

12. Retain unneeded accounts in a disabled state in accordance with the agency's records retention policy.

13. Configure applications to clear cached data and temporary files upon exit of the application or logoff of the system.

14. Associate access levels with group membership, where practicable, and require that every IT system user account be a member of at least one user group.

15. Require that the System Owner and the System Administrator investigate any unusual IT system access activities and approve changes to access level authorizations.

16. Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.

17. Require that local administrator rights, or the equivalent on non-Microsoft Windows-based IT systems, be granted only to authorized IT staff.

18. Require that at least two individuals have administrative accounts to each IT system, to provide continuity of operations.

For internal IT systems:

19. Require a documented request from the user to establish an account on any internal IT system.

20. Complete any agency-required background check before establishing accounts, or as soon as practicable thereafter.

21. Require employee job descriptions that accurately reflect assigned duties and responsibilities in order to define required IT system access.

22. Require confirmation of the account request and approval by the IT system user's supervisor and approval by the System Owner to establish accounts for sensitive IT systems.

23. Require delivery of access credentials to the user based on information already on file.

24. Notify supervisors, Human Resources, and the System Administrator in a timely manner about termination, transfer of employees and contractors with access rights to internal IT systems and data.

For customer-facing IT systems:

25. Require secure delivery of access credentials to users of all customer-facing IT systems.

26. Require confirmation of the user's request for access credentials based on information already on file prior to delivery of the access credentials to users of sensitive, customer-facing IT systems.

27. Require delivery of access credentials to users of customer-facing sensitive IT systems by means of an alternate channel (i.e., U.S. Mail).

5.3 Password Management

5.3.1 Purpose

Password Management requirements specify the means for password use to protect IT systems and data.

5.3.2 Requirements

Each agency shall or shall require that its service provider document formal password management practices. At a minimum, these practices shall include the following components:

1. Require the use of non-shared and a unique password on all accounts on IT systems classified as sensitive, including local, remote access and temporary accounts.

2. Require passwords on mobile devices issued by the agency such as PDAs and smart phones. For mobile phones, use a 4 to 5 digit pin number.

3. Require password complexity

   - at least eight characters in length,
   - not be based on a single dictionary word (ex. Bad Password: P4$sw0rD vs. Good Password: t0YtR4p!), and utilize at least three of the following four:

   - special characters,
   - alphabetical characters,
   - numerical characters,
   - combination of upper case and lower case letters.

4. Require that default passwords be changed immediately after installation.

5. Prohibit the transmission of identification and authentication data (e.g., passwords) without the use of industry accepted encryption standards (see Section 6.3 – Encryption).

6. Require IT system users to maintain exclusive control and use of their passwords, to protect them from inadvertent disclosure to others.

7. Configure sensitive IT systems to allow users to change their password at will.

8. Require users of sensitive IT systems to include network systems to change their passwords after a period of 42 days.

   Note: The Center for Internet Security are moving to 42 days = 6 weeks, notifications can begin 2 weeks out - thus the user gets a 30 day password rotation for those that change at the first notification.

9. Require that IT system users immediately change their passwords and notify the ISO if they suspect their passwords have been compromised.

10. Maintain the last 24 passwords used in the password history files to prevent the reuse of the same or similar passwords, commensurate with sensitivity and risk.

    Note: Reference CIS standards for Windows - http://www.cisecurity.org/tools2/windows/CIS_Win2003_DC_Benchmark_v2.0.pdf

11. Provide a unique initial password for each new user of sensitive IT systems, deliver the initial password to the IT system user in a secure and confidential manner, and require that the IT system user change the initial password upon the first login attempt.

12. Require that forgotten initial passwords be replaced rather than reissued.

13. Prohibit group account IDs and shared passwords on sensitive IT systems.

14. Prohibit the storage of passwords in clear text.

15. Limit access to files containing passwords to the IT system and its administrators.

16. Suppress the display of passwords on the screen as they are entered.

17. Implement a screen saver lockout period after a maximum of 30 minutes of inactivity for COV devices. COV devices with access to sensitive systems or those devices in less physically secure environments must have a lower time out interval documented and enforced.

18. Determine requirements for hardware passwords based on sensitivity and risk

19. Document and store hardware passwords securely.

20. Implement procedures to handle lost or compromised passwords and/or tokens.

5.4 Remote Access

5.4.1 Purpose

Remote Access requirements identify the steps necessary to provide for the secure use of remote access within the COV enterprise network.

5.4.2 Requirements

Commensurate with sensitivity and risk, each agency shall or shall require that its service provider:

1. Protect the security of all remote access to the agency's sensitive IT systems and data by means of encryption, in a manner consistent with Section 6.3.

   Note: This encryption requirement applies both to session initiation (i.e., identification and authentication) and to all exchanges containing sensitive data.

2. Protect the security of remote file transfer of sensitive data to and from COV IT systems by means of encryption, in a manner consistent with Section 6.3.

3. Document requirements for use of remote access and for remote access to sensitive data, based on agency and COV policies, standards, guidelines, and procedures.

4. Require that IT system users obtain formal authorization and a unique user ID and password prior to using the agency's remote access capabilities.

5. Document requirements for the physical and logical hardening of remote access devices.

6. Require maintenance of auditable records of all remote access.

6. DATA PROTECTION

6.1 Purpose

Data Protection requirements delineate the steps necessary to protect COV data from improper or unauthorized disclosure. This component of the COV IT Security Program defines requirements in the following two areas:

- Data Storage Media Protection
- Encryption

6.2 Data Storage Media Protection

6.2.1 Purpose

Data Storage Media Protection requirements identify the steps necessary for the appropriate handling of stored data to protect the data from compromise.

6.2.2 Requirements

Each agency shall or shall require that its service provider document Data Storage Media protection practices. At a minimum, these practices must include the following components:

1. Define protection of stored sensitive data as the responsibility of the Data Owner.

2. Prohibit the storage of sensitive data on any non-network storage device or media, except for backup media, unless the data is encrypted and there is a written exception approved by the Agency Head that includes the following elements:
   a. The business or technical justification;
   b. The scope, including quantification and duration (not to exceed one year);
   c. A description of all associated risks;

d. Identification of controls to mitigate the risks, one of which must be encryption; and
e. Identification of any unmitigated risks.

Note: Non-network storage device or media, includes removable data storage media and the fixed disk drives of all desktops and mobile workstations, such as laptop and tablet computers, USB drives, CDs, etc.

3. Require logical and physical protection for all data storage media containing sensitive data, commensurate with sensitivity and risk.

4. Prohibit the connection of any non-COV owned data storage media or device to a COV-owned network, unless the connection is to a segmented guest network. This prohibition, at the agency's discretion, need not apply to an approved vendor providing operational IT support services under contract.

Note: Such media include, but are not limited to, USB drives, cell phones, personal digital assistants, desktops, laptops, and digital music players owned by employees, contractors, and students.

5. Prohibit the auto forwarding of emails to external accounts to prevent data leakage unless there is a documented business case disclosing unmitigated risk approved in writing by the Agency Head.

6. Restrict the pickup, receipt, transfer, and delivery of all data storage media containing sensitive data to authorized personnel.

7. Procedures must be implemented and documented to safeguard handling of all backup media containing sensitive data. Encryption of backup media shall be considered where the data is Personal Health Information (PHI), Personally Identifiable Information (PII), or Critical Infrastructure Information/Sensitive Security Information (CII/SSI). Where encryption is not a viable option, mitigating controls and procedures must be implemented and documented.

8. Implement processes to sanitize data storage media prior to disposal or reuse.

Note: Agencies should implement procedures to instruct Administrators and users on the disposal of data storage media when no longer needed in accordance with the current version of the *Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard* (COV ITRM Standard SEC514).

6.3 Encryption

6.3.1 Purpose

Encryption requirements provide a framework for selecting and implementing encryption controls to protect sensitive data. See section 9.4 for notification requirements regarding a breach of unencrypted sensitive data.

6.3.2 Requirements

Commensurate with sensitivity and risk, each agency shall:

1. Define and document agency practices for selecting and deploying encryption technologies and for the encryption of data.

2. Document appropriate processes before implementing encryption. These processes must include the following components:

    a. Instructions in the agency's IT Security Incident Response Plan on how to respond when keys are compromised;
    b. A secure key management system for the administration and distribution of encryption keys; and
    c. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances.

3. Require encryption during transmission of data that is sensitive relative to confidentiality and integrity.

7. FACILITIES SECURITY

7.1 Purpose

Facilities Security requirements identify the steps necessary to safeguard the physical facilities that house IT equipment, systems, services, and personnel.

7.2 Requirements

Commensurate with sensitivity and risk, each agency shall or shall require that its service provider document facilities security practices. These practices must include the following components, at a minimum:

1. Safeguard IT systems and data residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (such as mobile command centers).

2. Design safeguards to protect against human, natural, and environmental risks.

3. Require appropriate environmental controls such as electric power, heating, fire suppression, ventilation, air-conditioning and air purification, as required by the IT systems and data.

4. Protect against physical access by unauthorized personnel.

5. Control physical access to essential computer hardware, wiring, displays, and networks by the principle of least privilege.

6. Provide a system of monitoring and auditing physical access to sensitive IT systems.

7. Require that the ISO periodically review the list of persons allowed physical access to sensitive IT systems.

8. PERSONNEL SECURITY

8.1 Purpose

Personnel Security requirements delineate the steps necessary to restrict access to IT systems and data to those individuals who require such access as part of their job duties. This component of the COV IT Security Program defines requirements in the following three areas:

- Access Determination and Control
- Security Awareness and Training
- Acceptable Use

8.2 Access Determination and Control

8.2.1 Purpose

Access Determination and Control requirements identify the steps necessary to restrict access to IT systems and data to authorized individuals.

8.2.2 Requirements

Each agency shall or shall require that its service provider document access determination and control practices for all sensitive agency IT systems and all third-party IT systems with which sensitive agency IT systems interconnect. At a minimum, these practices shall include the following components:

1. Perform background investigations of all internal IT System users based on access to sensitive IT systems or data. Existing users may be grandfathered under the policy and may not be required to have background investigations.

   Note: Agencies should consult the *Code of Virginia* § 2.2-1201.1 and Department of Human Resource Management (DHRM) Policy 2.10.

2. Restrict visitor access to facilities that house sensitive IT systems or data.

3. Require non-disclosure and security agreements for access to IT systems and data, based on sensitivity and risk.

4. Remove physical and logical access rights upon personnel transfer or termination, or when requirements for access no longer exist, as required in Section 5.2 and Section 7.2.

5. Establish termination and transfer practices that require return of agency logical and physical assets that provide access to sensitive IT systems and data and the facilities that house them.

6. Temporarily disable physical and logical access rights when personnel are not working for a prolonged period in excess of 30 days due to leave, disability or other authorized purpose.

7. Disable physical and logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.

8. Establish separation of duties in order to protect sensitive IT systems and data, or establish compensating controls when constraints or limitations of the agency prohibit a complete separation of duties.

Example: Such compensating controls may include increased supervisory review; reduced span of control; rotation of assignments; independent review, monitoring, and/or auditing; and timed and specific access authorization with audit review, among others.

9. Explicitly grant physical and logical access to sensitive IT systems and data and the facilities that house them based on the principle of least privilege.

8.3 IT Security Awareness and Training

8.3.1 Purpose

Security Awareness and Training requirements identify the steps necessary to provide IT system managers, administrators, and users with awareness of system security requirements and of their responsibilities to protect IT systems and data.

8.3.2 Requirements

Each agency shall:

1. Designate an individual who is responsible for all aspects of an agency's security awareness and training program including development, implementation, testing, training, monitoring attendance, and periodic updates.

2. Include any agency-specific IT security training requirements in the agency IT security awareness and training program.

   Example: An agency that processes data covered by the Health Insurance Portability and Accountability Act (HIPAA) must have an IT security training program that addresses specific HIPAA data security requirements.

3. Require that all IT system users, including employees and contractors, receive IT security awareness training annually, or more often as necessary.

4. Provide additional role-based IT security training commensurate with the level of expertise required for those employees and contractors who manage, administer, operate, and design IT systems, as practicable and necessary.

   Example: Agency employees and contractors who are members of the Disaster Recovery Team or Incident Response Team require specialized training in these duties.

5. Implement processes to monitor and track completion of IT security training.

6. Require IT security training before (or as soon as practicable after) IT system users receive access rights to the agency's IT systems, and in order to maintain these access rights.

7. Develop an IT security training program so that each IT system user is aware of and understands the following concepts:

   a. The agency's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;
   b. The concept of separation of duties;
   c. Prevention and detection of IT security incidents, including those caused by malicious code;

d. Proper disposal of data storage media;
e. Access controls, including creating and changing passwords and the need to keep them confidential;
f. Agency acceptable use policies;
g. Agency Remote Access policies; and
h. Intellectual property rights, including software licensing and copyright issues.

Note: Over a period of years, security awareness training should include the concepts above based on the needs of the agency relative to the sensitivity of the agency's data and IT systems.

8. Require documentation of IT system users' acceptance of the agency's security policies after receiving IT security training.

9. Require specialized IT security training for agency employees, contractors, vendors, business partners, and third parties with specific IT security duties beyond those of all IT systems users as practicable and necessary, including:

a. System Owners, Data Owners, and System Administrators;
b. IT Disaster Recovery team members; and
c. IT Security Incident Response Team members.

8.4 Acceptable Use

8.4.1 Purpose

Acceptable Use requirements identify the steps necessary to define acceptable and permitted use of IT systems.

8.4.2 Requirements

Each agency shall:

1. Document an agency acceptable use policy. Executive branch agencies must adhere to Virginia Department of Human Resource Management *Policy 1.75 – Use of Internet and Electronic Communication Systems.* Each Executive branch agency shall supplement the policy as necessary to address specific agency needs.

Note: This policy can be found at http://www.dhrm.virginia.gov/hrpolicy/policy/pol1_75.pdf.

2. Inform IT system users that the COV reserves the right (with or without cause) to monitor, access, and disclose all data created, sent, received, processed, or stored on COV systems.

3. Limit Local Administrator rights, or the equivalent on non-Microsoft Windows-based IT systems, to only authorized IT staff, as stated in 5.2.2, #18, so as to prevent users from:

a. Installing or using proprietary encryption hardware/software on COV owned systems;
b. Tampering with security controls configured on their workstations;
c. Installing personal software on a COV owned system;
d. Adding hardware to, removing hardware from, or modifying hardware on a COV system; and

e. Connecting non-COV-owned devices to a COV IT system or network, such as personal computers, laptops, or hand held devices, except in accordance with the current version of the *Use of non-Commonwealth Computing Devices to Telework Standard (*COV ITRM Standard SEC511*).*

4. Prohibit the use of copyrighted and licensed materials on COV systems unless the COV owns the materials or COV has otherwise complied with intellectual property laws governing the materials.

5. Prohibit the transmission of unencrypted sensitive data over the Internet.

6. Require documentation of IT system users' acceptance of the agency's Acceptable Use Policy before, or as soon as practicable after, gaining access to agency IT systems.

8.5.1. Email Communications

8.5.2. *Purpose*

Email shall not be used to send sensitive data unless there is encryption. As stated in section 6.3.2 of this standard, encryption is required for the transmission of data that is sensitive relative to confidentiality and integrity. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus. An email disclaimer is a set of statements that are either pre-pended or appended to emails. These statements are frequently used to create awareness of how to treat the data in the email. An email disclaimer is not a substitute for judgment on what content to put into an email.

8.5.3. Email Disclosure Requirements

The ISO must consult with the agency's legal counsel before adopting an email disclaimer. Emails sent from Commonwealth systems are public records of the Commonwealth of Virginia and must be managed as such. Following is an example of an email disclaimer for consideration when meeting with your agency's legal counsel.

The information in this email and any attachments may be confidential and privileged. Access to this email by anyone other than the intended addressee is unauthorized. If you are not the intended recipient (or the employee or agent responsible for delivering this information to the intended recipient) please notify the sender by reply email and immediately delete this email and any copies from your computer and/or storage system. The sender does not authorize the use, distribution, disclosure or reproduction of this email (or any part of its contents) by anyone other than the intended recipient(s).

No representation is made that this email and any attachments are free of viruses. Virus scanning is recommended and is the responsibility of the recipient.

9. THREAT MANAGEMENT

9.1 Purpose

Threat Management delineates the steps necessary to protect IT systems and data by preparing for and responding to IT security incidents. This component of the COV IT Security Program defines requirements in the following four areas:

- Threat Detection
- IT Security Monitoring and Logging
- IT Security Incident Handling
- Data Breach Notification

9.2 Threat Detection

9.2.1 Purpose

Threat Detection requirements identify the practices for implementing intrusion detection and prevention.

9.2.2 Requirements

Each agency shall or shall require that its service provider document threat detection practices that include the following components, at a minimum:

1. Designate an individual responsible for the agency's threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance.

2. Conduct Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) log reviews to detect new attack patterns as quickly as practicable.

3. Develop and implement required mitigation measures based on the results of IDS and IPS log reviews.

4. Maintain regular communication with security research and coordination organizations, such as US CERT, to obtain information about new attack types, vulnerabilities, and mitigation measures.

9.3 IT Security Monitoring and Logging

9.3.1 Purpose

IT Security Monitoring and Logging requirements identify the steps necessary to monitor and record IT system activity.

9.3.2 Requirements

Commensurate with sensitivity and risk, each agency shall, or shall require that its service provider, document IT security monitoring and logging practices that include the following components, at a minimum:

1. Designate individuals responsible for the development and implementation of IT security logging capabilities, as well as detailed procedures for reviewing and administering the logs.

2. Enable logging on all IT systems.

3. Monitor IT system event logs in real time, correlate information with other automated tools, identifying suspicious activities, and provide alert notifications.

4. Document standards that specify the type of actions an IT system should take when a suspicious or apparent malicious activity is taking place.

Example: Possible actions include stopping the event, shutting down the IT system, and alerting appropriate staff.

Note: Multiple actions may be warranted and advisable, based on sensitivity and risk.

5. Prohibit the use of keystroke logging, except when required for security investigations and approved in writing by the Agency Head.

9.4 IT Security Incident Handling

9.4.1 Purpose

IT Security Incident Handling requirements identify the steps necessary to respond to suspected or known breaches to IT security safeguards.

9.4.2 Requirements

Each agency shall document IT security incident handling practices and where appropriate the agency shall incorporate its service provider's procedures for incident handling practices that include the following components, at a minimum:

1. Designate an IT Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber attacks.

2. Identify controls to deter and defend against cyber attacks to best minimize loss or theft of information and disruption of services.

3. Implement proactive measures based on cyber attacks to defend against new forms of cyber attacks.

4. Establish IT security incident categorization and prioritization based on the immediate and potential adverse effect of the IT security incident and the sensitivity of affected IT systems and data.

5. Identify immediate mitigation procedures, including specific instructions, based on IT security incident categorization level, on whether or not to shut down or disconnect affected IT systems.

6. Establish a process for reporting IT security incidents to the CISO. Executive branch agencies must establish a reporting process for IT security incidents in accordance with §2.2-603(F) of the *Code of Virginia* so as to report "*to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence*," "*all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities.*"

7. Establish requirements for internal agency IT security incident recording and reporting requirements, including a template for the incident report.

8. Establish procedures for IT security incident investigation, preservation of evidence, and forensic analysis.

9. Report IT security incidents only through channels that have not been compromised.

9.5 Data Breach Notification

9.5.1 Purpose

To specify the notification requirements for agencies by identifying the triggering factors and necessary responses to unauthorized release of unencrypted sensitive information.

9.5.2 Requirements

Each agency shall:

1. Identify all agency systems, processes, and logical and physical data storage locations (whether held by the agency or a third party) that contain Personal Information which means the first name or first initial and last name in combination with and linked to any one or more of the following data elements, when the data elements are neither encrypted nor redacted.
    a. Social security number
    b. Drivers license number or state identification card number issued in lieu of a driver's license number.
    c. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts..
    d. Other personal identifying information, such as insurance data or date of birth.

    "Redact" means alteration or truncation of data such that no more than the following are accessible as part of the information:
    a. Five digits of a social security number; or
    b. The last four digits of a driver's license number, state identification card number, or account number.

    Note: The term does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.

2. Include provisions in any third party contracts requiring that the third party and third party subcontractors:
    a. Provide immediate notification to the agency of suspected breaches; and

    b. Allow the agency both to participate in the investigation of incidents and exercise control over decisions regarding external reporting.

3. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted and/or un-redacted Personal Information by any mechanism, including, but not limited to:

    a. Theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's, tapes, USB drives, SD cards, etc.
    b. Theft or loss of physical hardcopy
    c. Security compromise of any system.

An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.

If a data custodian is the entity involved in the data breach they must alert the data owner so that the data owner can notify the affected individuals.

The agency shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #8, below.

4. In the case of a computer found to be infected with malware that exposes data to unauthorized access, individuals that may have had their information exposed due to use of that computer must be alerted in accordance with data breach rules.

5. Provide notification that consists of:

    a. A general description of what occurred and when;
    b. The type of personal information that was involved;
    c. What actions have been taken to protect the individual's personal information from further unauthorized access;
    d. A telephone number that the person may call for further information and assistance, if one exists; and
    e. What actions the agency recommends that the individual take. The actions recommended should include monitoring their credit report and reviewing their account statements.

6. Provide this notification by one or more of the following methodologies, listed in order of preference:
    a. Written notice to the last known postal address in the records of the individual or entity;
    b. Telephone Notice;
    c. Electronic notice; or
    d. Substitute Notice - if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice. Substitute notice consists of all of the following:
        i. Email notice if the individual or the entity has email addresses for the members of the affected class of residents;
        ii. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and
        iii. Notice to major statewide media.

7. In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to section E. of Code of Virginia, §18.2-186.6, the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C.§1681(a)(p), of the timing, distribution, and content of the notice.

8. Not provide notification immediately following verification of unauthorized data disclosure only if law-enforcement is notified and the law-enforcement agency determines and advises the individual or entity that the notice would impede a criminal or civil investigation, or homeland security or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no long impede the investigation or jeopardize national or homeland security.

10. IT ASSET MANAGEMENT

10.1 Purpose

IT Asset Management delineates the steps necessary to protect IT systems and data by managing the IT assets themselves in a planned, organized, and secure fashion. This component of the COV IT Security Program defines requirements in the following three areas:

- IT Asset Control
- Software License Management
- Configuration Management and Change Control

10.2 IT Asset Control

10.2.1 Purpose

IT Asset Control requirements identify the steps necessary to control and collect information about IT assets.

10.2.2 Requirements

Commensurate with sensitivity and risk, each agency shall or shall require that its service provider document inventory management practices that address the following components, at a minimum:

1. Identify whether IT assets may be removed from premises that house IT systems and data, and if so, identify the controls over such removal.

2. Identify whether personal IT assets are allowed onto premises that house IT systems and data, and if so, identify the controls necessary to protect these IT systems and data.

3. Remove data from IT assets prior to disposal in accordance with the current version of the *Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard* (COV ITRM Standard SEC514).

4. Require creation and periodic review of a list of agency hardware and software assets.

10.3 Software License Management

10.3.1 Purpose

Software License Management requirements identify the steps necessary to protect against use of computer software in violation of applicable laws.

10.3.2 Requirements

Each agency shall or shall require that its service provider document software license management practices that address the following components, at a minimum:

1. Require the use of only agency approved software on IT systems.

2. Assess periodically whether all software is used in accordance with license agreements.

10.4 Configuration Management and Change Control

10.4.1 Purpose

Configuration Management and Change Control requirements identify the steps necessary to document and monitor the configuration of IT systems, and to control changes to these items during their lifecycles. While the full extent of Configuration Management and Change Control is beyond the scope of this document, Agencies are advised to institute structured practices in this area, based on industry standard frameworks such as the IT Infrastructure Library (ITIL) (www.itil.co.uk) or Control Objectives for Information and related Technology (COBIT) (www.isaca.org), among others.

10.4.2 Requirements

Each agency shall, or shall require that its service provider, document configuration management and change control practices so that changes to the IT environment do not compromise IT security controls.

This page intentionally left Blank

GLOSSARY OF IT SECURITY DEFINITIONS

Academic Instruction and Research Systems: Those systems used by institutions of higher education for the purpose of providing instruction to students and/or by students and/or faculty for the purpose of conducting research.

Access: Access: The ability to use, modify or affect an IT system or to gain entry to a physical area or location.

Access Controls: Access controls: A set of security procedures that monitor access and either allow or prohibit users from accessing IT systems and data. The purpose of access controls is to prevent unauthorized access to IT systems.

Accountability: The association of each log-on ID with one and only one user, so that the user can always be tracked while using an IT system, providing the ability to know which user performed what system activities.

Agency Head: The chief executive officer of a department established in the government of the Commonwealth of Virginia.

Alert: Notification that an event has occurred or may occur.

Alternate Site: A location used to conduct essential business functions in the event that access to the primary facility is denied or the primary facility has been so damaged as to be unusable.

Application: A computer program or set of programs that meet a defined set of business needs. See also *Application System.*

Application System: An interconnected set of IT resources under the same direct management control that meets a defined set of business needs. See also *Application, Support System,* and *Information Technology (IT) System.*

Asset: Any software, data, hardware, administrative, physical, communications, or personnel resource.

Assurance: Measurement of confidence in a control or activity.

Attack: An attempt to bypass security controls on an IT system in order to compromise the data.

Audit: An independent review and examination of records and activities to test for adequacy of controls, measure compliance with established policies and operational procedures, and recommend changes to controls, policies, or procedures.

Authentication: The process of verifying an identity of a user to determine the right to access specific types of data or IT system.

Authorization: The process of granting access to data or IT system by designated authority after proper identification and authentication.

Availability: Protection of IT systems and data so that they are accessible to authorized users when needed without interference or obstruction.

Backup: The process of producing a reserve copy of software or electronic files as a precaution in case the primary copy is damaged or lost.

Business Continuity Plan: A set of processes and procedures to recover an organization's essential business functions in a manner and on a schedule to provide for the ongoing viability of the organization if a disruption to normal operations occurs.

Baseline Security Configuration: The minimum set of security controls that must be implemented on all IT systems of a particular type.

Business Function: A collection of related structural activities that produce something of value to the organization, its stakeholders or its customers. See also *Essential Business Function.*

Business Impact Analysis (BIA): The process of determining the potential consequences of a disruption or degradation of business functions.

Change Control: A management process to provide control and traceability for all changes made to an application system or IT system.

Chief Information Officer of the Commonwealth (CIO): The CIO oversees the operation of the Virginia Information Technologies Agency (VITA) and, under the direction and control of the Virginia Information Technology Investment Board (the Board), exercises the powers and performs the duties conferred or imposed upon him by law and performs such other duties as may be required by the Board.

Chief Information Security Officer of the Commonwealth (CISO): The CISO is the senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of IT systems and data.

Commonwealth of Virginia (COV): The government of the Commonwealth of Virginia, and its agencies amd departments.

Commonwealth of Virginia Computer Incident Response Team (COV CIRT): A function of the Incident Management division of the COV Security and Risk Management directorate. The COV CIRT operates under the direction of the Incident Management Director, and is primarily comprised of the Incident Management engineers, with additional resources available as needed on a per incident basis from IT Partnership technical, legal and human resources staff.

Computer Emergency Response Team Coordination Center (CERT/CC): a center of Internet security expertise, located at the Software Engineering Institute at Carnegie Mellon University that studies Internet security vulnerabilities, researches long-term changes in networked systems, and develops information and training to assist the CERTs of other organizations. See also *Incident Response Team* and *United States Computer Emergency Response Team (US-CERT).*

Confidentiality: The protection of data from unauthorized disclosure to individuals or IT systems..

Configuration Management: A formal process for authorizing and tracking all changes to an IT system during its life cycle.

Continuity of Operations Planning: The process of developing plans and procedures to continue the performance of essential business functions in the event of a business interruption or threat of interruption.

Continuity of Operations Plan (COOP): A set of documented procedures developed to provide for the continuance of essential business functions during an emergency.

Control Objectives for Information and related Technology (COBIT): A framework of best practices (framework) for IT management that provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control.

Countermeasure: An action, device, procedure, technique, or other measure that reduces vulnerability or the impact of a threat to an IT system.

Credential: Information, such as a user ID and password passed from and IT system or IT system user to an IT system to establish access rights.

Cryptography: The process of transforming plain text into cipher text, and cipher text into plain text.

Customer-Facing IT System: An IT system designed and intended for by external agency customers and or by the public. COV employees, contractors, and business partners may also use such systems. See also IT System and Internal IT System.

Data: An arrangement of numbers, characters, and/or images that represent concepts symbolically...

Database: A collection of logically related data (and a description of this data), designed to meet the information needs of an organization.

Data Classification: A process of categorizing data according to its sensitivity.

Data Custodian: An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

Data Owner: An agency Manager, designated by the Agency Head or Information Security Officer, who is responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data.

Data Security: Data Security refers to those practices, technologies, and/or services used to apply security appropriately to data.

Data Sensitivity: See Sensitivity.

Digital Certificate: An electronic document attached to a file that certifies the file is from the organization it claims to be from and has not been modified from the original format.

Digital Signature: A number that uniquely identifies the sender of a message and proves the message is unchanged since transmission.

Disaster Recovery Plan (DRP): A set of documented procedures that identify the steps to restore essential business functions on a schedule that supports agency mission requirements.

Data Storage Media: A device used to store IT data. Examples of data storage media include floppy disks, fixed disks, CD-ROMs, and USB flash drives.

Electronic Information: Any information stored in a format that enables it to be read, processed, manipulated, or transmitted by an IT system.

Encryption: The process or the means of converting original data to an unintelligible form so it cannot be read by unauthorized users..

Essential Business Function: A business function is essential if disruption or degradation of the function prevents the agency from performing its mission as described in the agency mission statement.

Evaluation: Procedures used in the analysis of security mechanisms to determine their effectiveness and to support or refute specific system weaknesses.

Extranet: A trusted network; used by COV to connect to a third-party provider.

Federal Information Security Management Act (FISMA): Federal legislation whose primary purpose is to provide a comprehensive framework for IT security controls in Federal agencies.

Firewall: Traffic-controlling gateway that controls access, traffic, and services between two networks or network segments, one trusted and the other untrusted.

Function: A purpose, process, or role.

Fuzz Testing: This is a software testing technique that provides random data ("fuzz") to the inputs of a program. If the program fails (for example, by crashing, or by failing built-in code assertions), the defects can be noted.

Group: A named collection of IT system users; created for convenience when stating authorization policy.

Group-based Access: Authorization to use an IT system and/or data based on membership in a group.

Harden: The process of implementing software, hardware, or physical security controls to mitigate risk associated with COV infrastructure and/or sensitive IT systems and data.

High Availability: A requirement that the IT system is continuously available, has a low threshold for down time, or both.

Identification: The process of associating a user with a unique user ID or login ID.

Incident Response Capability (IRC): The follow-up to an incident including reporting, responding and recovery procedures.

Information: Data organized in a manner to enable their interpretation.

Information Security Officer (ISO): The individual designated by the Agency Head to be responsible for the development, implementation, oversight, and maintenance of the agency's IT security program.

Information Technology (IT): Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology (IT) Assurance: Measures that protect and defend information and IT systems by providing for their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Technology (IT) Contingency Planning: The component of Continuity of Operations Planning that prepares for continuity and/or recovery of an organization's IT systems and data that support its essential business functions in the event of a business interruption or threat of interruption.

Information Technology (IT) Infrastructure Library (ITIL): A framework of best practice processes designed to facilitate the delivery of high quality information technology (IT) services.

Information Technology (IT) Security: The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality.

Information Technology (IT) Security Architecture: The logical and physical security infrastructure made up of products, functions, locations, resources, protocols, formats, operational sequences, administrative and technical security controls, etc., designed to provide the appropriate level of protection for IT systems and data.

Information Technology (IT) Security Audit: The examination and assessment of the adequacy of IT system controls and compliance with established IT security policy and procedures.

Information Technology (IT) Security Auditor: CISO personnel, agency Internal Auditors, the Auditor of Public Accounts, or a private firm that, in the judgment of the agency, has the experience and expertise required to perform IT security audits.

Information Technology (IT) Security Breach: The violation of an explicit or implied security policy that compromises the integrity, availability, or confidentiality of an IT system.

Information Technology (IT) Security Controls: The protection mechanisms prescribed to meet the security requirements specified for an IT system.

IT Security Event: An occurrence that has yet to be assessed but may affect the performance of an IT system.

Information Technology (IT) Security Incident: An adverse event or situation, whether intentional or accidental, that poses a threat to the integrity, availability, or confidentiality of an IT system.

Information Technology (IT) Security Incident Response Team: An organization within an agency constituted to monitor IT security threats and prepare for and respond to cyber attacks. See also *Computer Emergency Response Team Coordination Center (CERT/CC)* and *United States Computer Emergency Response Team (US-CERT).*

Information Technology (IT) Security Logging: Chronological recording of system activities sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to its final results.

Information Technology (IT) Security Policy: A statement of the IT Security objectives of an organization, and what employees, contractors, vendors, business partners, and

third parties of the organization must do to achieve these objectives.

Information Technology (IT) Security Program: A collection of security processes, standards, rules, and procedures that represents the implementation of an organization's security policy

Information Technology (IT) Security Requirements: The types and levels of protection necessary to adequately secure an IT system.

Information Technology (IT) Security Safeguards: See *Information Technology (IT) Security Controls*.

Information Technology (IT) Security Standards: Detailed statements of how employees, contractors, vendors, business partners, and third parties of an organization must comply with its IT Security policy.

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control. See also *Application System* and *Support System.*

Information Technology (IT) System Sensitivity: See Sensitivity.

Information Technology (IT) System Users: As used in this document, a term that includes COV employees, contractors, vendors, third-party providers, and any other authorized users of IT systems, applications, telecommunication networks, data, and related resources.

Integrity: The protection of data or IT system from intentional or accidental unauthorized modification.

Internal IT System: An IT system designed and intended for use only by COV employees, contractors, and business partners. See also IT System and Customer-Facing IT System.

Internal IT System User: A member of the agency workforce who uses an IT system in any capacity to perform the duties of their position.

Internet: An external worldwide public data network using Internet protocols to which COV can establish connections.

Intranet: A trusted multi-function (data, voice, video, image, facsimile, etc.) private digital network using Internet protocols, which can be developed, operated and maintained for the conduct of COV business.

Intrusion Detection: A method of monitoring traffic on the network to detect break-ins or break-in attempts, either manually or via software expert systems.

Intrusion Detection Systems (IDS): Software that detects an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

Intrusion Prevention Systems (IPS): Software that prevents an attack on a network or computer system. An IPS is a significant step beyond an IDS (intrusion detection system), because it stops the attack from damaging or retrieving data. Whereas an IDS passively monitors traffic by sniffing packets off of a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets. It can thus block attacks in real time.

ISO/IEC 17799: An IT security standard published in 2005 by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). It provides best practice recommendations on IT security management for use by those who are responsible for initiating, implementing or maintaining information security management systems.

Key: A sequence of data used in cryptography to encrypt or decrypt information

Key Escrow: The process of storing the encryption key with a third-party trustee to allow the recovery of encrypted text.

Least Privilege: The minimum level of data, functions, and capabilities necessary to perform a user's duties.

Logon ID: An identification code (normally a group of numbers, letters, and special characters) assigned to a particular user that identifies the user to the IT system.

Malicious Code: Harmful code (such as viruses and worms) introduced into a program or file for the purpose of contaminating, damaging, or destroying IT systems and/or data. Malicious code includes viruses, Trojan horses, trap doors, worms, spy-ware, and counterfeit computer instructions (executables)..

Malicious Software: See Malicious Code.

Management Control: A set of mechanisms designed to manage organizations to achieve desired objectives.

Mission Critical Facilities: The data center's physical surroundings as well as data processing equipment inside and the systems supporting them that need to be secured to achieve the availability goals of the system function.

Monitoring: Listening, viewing, or recording digital transmissions, electromagnetic radiation, sound, and visual signals.

Non-repudiation: A characteristic of a message that validates that the message was sent by a particular organization or individual, and cannot be refuted.

Off-site Storage: The process of storing vital records in a facility that is physically remote from the primary site. To qualify as off-site, the facility should be geographically/separately and distinct from the primary site and offer environmental and physical access protection.

Operational Controls: IT security measures implemented through processes and procedures.

Operational Risk: The possibility of loss from events related to technology and infrastructure failure, from business interruptions, from staff related problems and from external events such as regulatory changes.

Out-of-Band Communications: A secondary communications channel for emergencies and/or redundancy.

Password: A unique string of characters that, in conjunction with a logon ID, authenticates a user's identity.

Penetration testing: A penetration test is a method of evaluating the security computer system or network simulating an attack by a malicious user.

Personal Digital Assistant (PDA): A digital device, which can include the functionality of a computer, a cellular telephone, a music player and a camera

Personal Identification Number (PIN): A short sequence of digits used as a password.

Personal Information: "Personal information" means all information that describes, locates or indexes anything about an individual including his real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution. "Personal information" shall not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information. *Code of Virginia* § 2.2-3801.

Personally Identifiable Information (PII): Any piece of information that can potentially be used to uniquely identify, contact, or locate a single person.

Personnel: All COV employees, contractors, and subcontractors, both permanent and temporary.

Phishing: A form of criminal activity characterized by attempts to acquire sensitive information fraudulently, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication.

Privacy: The rights and desires of an individual to limit the disclosure of individual information to others.

Privacy Officer: The privacy officer, if required by statute (such as HIPPA) provides guidance on the requirements of state and federal Privacy laws; disclosure of and access to sensitive data; and security and protection requirements in conjunction with the IT system when there is some overlap among sensitivity, disclosure, privacy, and security issues.

Public web site: A public web site is the most visible and readily accessible to the average Web user. A site on the Web that is accessible by anyone with a Web browser and access to the Internet.

Risk: The potential that an event may cause a material negative impact to an asset.

Risk Analysis: A systematic process to identify and quantify risks to IT systems and data and to determine the probability of the occurrence of those risks.

Risk Management: Identification and implementation of IT security controls in order to reduce risks to an acceptable level.

Recovery: Activities beyond the initial crisis period of an emergency or disaster that are designed to return IT systems and/or data to normal operating status.

Residual Risk: The portion of risk that remains after security measures have been applied.

Restoration: Activities designed to return damaged facilities and equipment to an operational status.

Risk: The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result.

Risk Assessment (RA): The process of identifying and evaluating risks so as to assess their potential impact..

Risk Mitigation: The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk.

Role-based Access Control: A type of access control in which IT system users receive access to the IT systems and data based on their positions or roles in an organization.

Roles and Responsibility: Roles represent a distinct set of operations and responsibilities required to perform some particular function that an individual may be assigned. Roles may differ from the individual's business title. This document contains the roles and responsibilities associated with implementing IT security.

Recovery Point Objective (RPO): The measurement of the point in time to which data must be restored in order to resume processing transactions. Directly related to the amount of data that can be lost between the point of recovery and the time of the last data backup

Recovery Time Objective (RTO): The period of time in which systems, applications or functions must be recovered after an outage. .

Secure: A state that provides adequate protection of IT systems and data against compromise, commensurate with sensitivity and risk.

Sensitive: See Sensitivity.

Sensitivity: A measurement of adverse affect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled that compromise of IT systems and data with respect to confidentiality, integrity, and/or availability could cause.. IT systems and data are sensitive in direct proportion to the materiality of the adverse effect caused by their compromise.

Sensitivity Classification: The process of determining whether and to what degree IT systems and data are sensitive.

Separation of Duties: Assignment of responsibilities such that no one individual or function has control of an entire process. It is a technique for maintaining and monitoring accountability and responsibility for IT systems and data.

Shared Accounts: A logon ID or account utilized by more than one entity.

Source code auditing: A software (source) code audit is a comprehensive analysis of source code in a programming project with the intent of discovering bugs, security breaches or violations of programming conventions. It is an integral part of the defensive programming paradigm, which attempts to reduce errors before the software is released.

Spy-ware: A category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

State: See *Commonwealth of Virginia (COV).*

Support System: An interconnected set of IT resources under the same direct management control that shares common functionality and provides services to other systems. See also *Application System* and *Information Technology (IT) System.*

System. See *Information Technology (IT) System*

System Administrator: An analyst, engineer, or consultant who implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian.

System Owner: An agency Manager, designated by the Agency Head or Information Security Officer, who is responsible for the operation and maintenance of an agency IT system.

Technical Controls: IT security measures implemented through technical software or hardware.

Third-Party Provider: A company or individual that supplies IT equipment, systems, or services to COV Agencies.

Threat: Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Token: A small tangible object that contains a built-in microprocessor utilized to store and process information for authentication.

Trojan horse: A malicious program that is disguised as or embedded within legitimate software.

Trusted System or Network: An IT system or network that is recognized automatically as reliable, truthful, and accurate, without continual validation or testing.

United States Computer Emergency Response Team (US-CERT): A partnership between the Department of Homeland security and the public and private sectors, intended to coordinate the response to IT security threats from the Internet. As such, it releases information about current IT security issues, vulnerabilities and exploits as Cyber Security Alerts, and works with software vendors to create patches for IT security vulnerabilities. See also *Computer Emergency Response Team Coordination Center (CERT/CC)* and *Incident Response Team.*

Universal Serial Bus (USB): A standard for connecting devices.

Untrusted: Characterized by absence of trusted status. Assumed to be unreliable, untruthful, and inaccurate unless proven otherwise.

USB Flash Drive: A small, lightweight, removable and rewritable data storage device.

User ID: A unique symbol or character string that is used by an IT system to identify a specific user. See Logon ID.

Virginia Department of Emergency Management (VDEM): A COV department that protects the lives and property of Virginia's citizens from emergencies and disasters by coordinating the state's emergency preparedness, mitigation, response, and recovery efforts

Version Control: A management process that provides traceability of updates to operating systems and supporting software.

Virus: See Malicious Code.

Virginia Information Technologies Agency (VITA): VITA is the consolidated, centralized IT organization for COV.

Vital Record: A document, regardless of media, which, if damaged or destroyed, would disrupt business operations.

Vulnerability: A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

Workstation: A terminal, computer, or other discrete resource that allows personnel to access and use IT resources.

IT SECURITY ACRONYMS

AITR: Agency Information Technology Representative

ANSI: American National Standards Institute

BIA: Business Impact Analysis

CAP: Corrective Action Plan

CIO: Chief Information Officer

CISO: Chief Information Security Officer

COOP: Continuity of Operations Plan

COPPA: Children's Online Privacy Protection Act

COTS: Council on Technology Services

DHRM: Department of Human Resource Management

DRP: Disaster Recovery Plan

FIPS: Federal Information Processing Standards

FISMA: Federal Information Security Management Act

FTP: File Transfer Protocol

HIPAA: Health Insurance Portability and Accountability Act

IDS: Intrusion Detection Systems

IPS: Intrusion Prevention Systems

IRC: Incident Response Capability

ISA: Interconnection Security Agreement

ISO: Information Security Officer

ITRM: Information Technology Resource Management

MOU: Memorandum of Understanding

OMB: Office of Management and Budget

PCI: Payment Card Industry

PDA: Personal Digital Assistant

PIA: Privacy Impact Assessment

PII: Personally Identifiable Information

PIN: Personal Identification Number

RA: Risk Assessment

RBD: Risk-Based Decisions

RPO: Recovery Point Objective

RTO: Recovery Time Objective

SLA: Service Level Agreement

SDLC: Systems Development Life Cycle

SNMP: Simple Network Management Protocol

SOP: Standard Operating Procedure

SSID: Service Set Identifier

SSP: Security Program Plan

ST&E: Security Test & Evaluation

ITIES: Information Technology Investment and Enterprise Solutions Directorate (VITA)

USCERT: Computer Emergency Response Team

VDEM: Virginia Department of Emergency Management

VITA: Virginia Information Technologies Agency

APPENDIX – IT SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM

The form an Agency must submit to request an exception to any requirement of this *Standard* and the related *IT Security Policy* is on the following page.

COV IT Security Policy & Standard Exception Request Form

Agency Name: _____Contact for Additional Information: _____

Requirement to which an exception is requested: _____

1. Provide the **Business or Technical Justification:**

2. Describe the scope including quantification and requested duration (not to exceed one (1) year):

3. Describe all associated risks:

4. Identify the controls to mitigate the risks:

5. Identify any unmitigated risks:

I have evaluated the business issues associated with this request and I accept any and all associated risks as being reasonable under the circumstances.

_____ _____ _____

Printed name Agency Head **Signature** **Date**

Chief Information Security Officer of the Commonwealth (CISO) Use Only

Approved_____ Denied_____ Comments:

_____ _____

CISO Date

Agency Request for Appeal Use Only

Approved_____ Comments:

_____ _____

Agency Head Date

Chief Information Officer of the Commonwealth (CIO) Office Use Only (Appeal)

Appeal Approved_____ Appeal Denied_____ Comments:

_____ _____

CIO Date